ISSN. 1363-6650

MARCH 1997
Issue 3

International Journal of FORENSIC COMPUTING™

Contents

International Journal of Forensic Computing
Third Floor, Colonnade House
High Street, Worthing, West Sussex
UK BN11 1NZ
Tel: +44 (0) 1903 209226
Fax: +44 (0) 1903 233545
e-mail: ijfc@pavilion.co.uk
http: //www.forensic-computing.com

Beyond Reasonable Confusion?

A fundamental issue under discussion at the moment centres on how the legal system can verify the accuracy of computer based evidence presented in court. The major difficulty appears to be that while computer expertise per se is relatively common, there are few formal qualifications in its practical application, and none in which it may be combined with awareness of forensic requirements. Computer based evidence requires special considerations during both collection and analysis, and technical experts should be aware of these. In order that Courts may correctly evaluate the evidence presented to them it is vital that both Prosecution and Defence work on identical copies of the original information.

The first and most contentious issue involves how evidence is gathered when equipment is seized for search. Since initial contact with the evidence is invariably the domain of the prosecution expert, it is here where proper guidelines are most urgently required. There are those who advocate the use of commercial disk editing programs like the Norton Utilities to search computer disks. However, regardless of the competence of the operator, the fact that such programs are capable of writing information to the disk places the evidence at risk of modification.

It is the job of a professional investigator to minimise all possible risks and since the accurate copying of information is now a relatively trivial task and can be completed without risk of modification, it is a measure of the professionalism of the investigator that he conducts his work on such a copy.

In this manner both Prosecution and Defence experts can work on identical material and any concern over the integrity of the evidence can be resolved by independent verification of the accuracy of the original copying process. Once material has been copied in this manner, subsequent work is much less sensitive to mistakes or potential logic bomb traps and in any case can be verified by reference to the original copy.

►

Articles are published on the understanding that publication is not taken to imply endorsement of the views therein by the Publisher or Editorial Team or members of the Advisory Board of the Journal. Courses of action described in the Journal in relation to one set of circumstances will not necessarily be appropriate for a different set of circumstances.

Accordingly, readers should take their own independent specialist advice before proceeding on any project or course of action and any failure to do so is at their own risk. No responsibility is assumed by the Publisher or Editorial Team or members of the Advisory Board for any loss or damage to persons or property as a matter of contract, negligence (save in respect of liability for death or personal injury arising out of any negligence) or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Whilst all reasonable care is taken, neither the Publisher, nor the Editorial Team, nor members of the Advisory Board can be held legally responsible for any errors in articles or listings. Upon submission of an article, the author will be requested to transfer copyright of the article to the Publisher.

A second issue is concerned with the technical competence of a computer expert. If the copying procedure described above is designed for non-technical use and is completed satisfactorily, the technical competence of the investigator subsequently has little bearing upon the acceptability of the factual evidence since any incompetence can be demonstrated by a parallel examination of the same material.

A recent case involved a logic bomb designed to delete certain files under a specific set of conditions, the logic bomb commands were in a batch file and the contents of this were produced in evidence. The prosecution expert produced an analysis of the action of the batch file which confirmed his assertion that recovery would have been costly and time consuming. A second prosecution witness who also had qualifications in computing technology agreed with the analysis. An independent expert was called in to check the report and found a fundamental error in the analysis which indicated that a full recovery could have been completed in minutes.

A related aspect of technical competence is how an expert chooses to present his observations for the consideration of the Court. Within Criminal Law in the United Kingdom, this seems to be a most difficult area since it centres around the fundamental concept of guilt being established "beyond reasonable doubt".

In a prosecution for Blackmail, much of the evidence was recovered from computer disks and was presented in a report by a competent police officer. The Defence produced a voluminous technical report which attempted to challenge the technical accuracy of the copying process on the basis of the format that the information was in when the defence expert examined it. At no point did this report challenge the validity of the presented evidence.

In a case brought under the Computer Misuse Act (1990) the defence expert began his report by criticising the wording of the charge on the basis that a 3.5" disk was not "floppy" because it was contained in a rigid plastic envelope. To anyone with even slight knowledge of computers such observations are frivolous but in less obvious cases the Court may not be aware of this and gratuitous confusion can be introduced quite deliberately in order to cloud the issues under consideration.

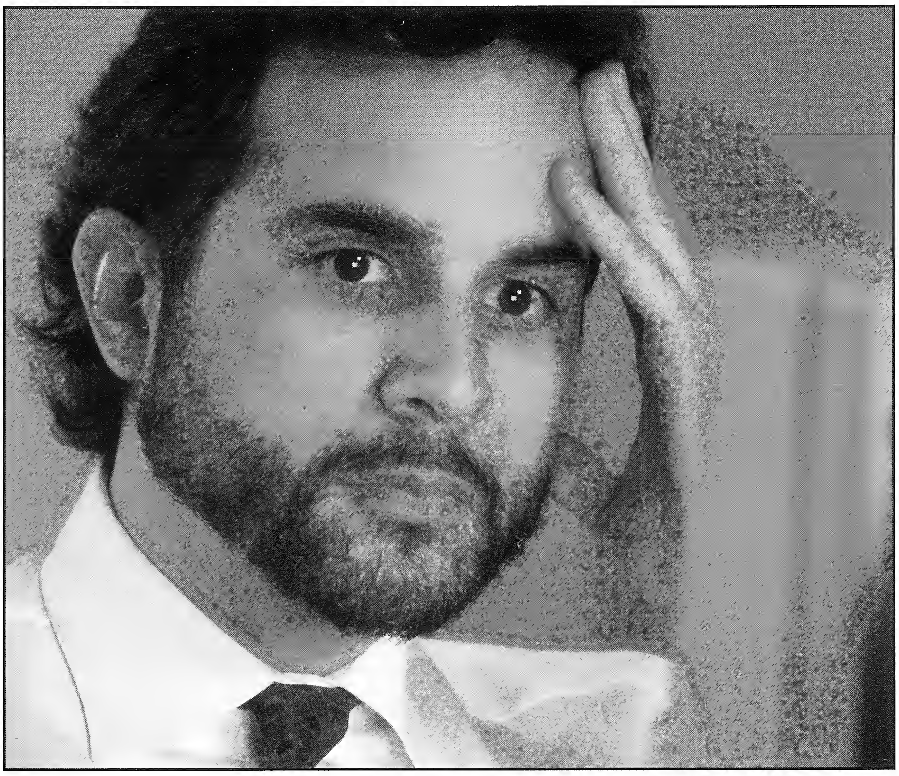
Another aspect worthy of mention is that involvement in the commission of particular computer crime, by the perceived mystique of computer technology, is assumed to be a qualification for expertise in general computer forensics.

It is thus apparent that some method of determining the competence and integrity of technical experts is urgently required. There appear to be no academic examinations or qualifications available and few formal training opportunities.

It may be that publication of a series of guidelines would be a useful start, followed perhaps by the introduction of a category dealing with computer based material within one of the existing Forensic Service divisions.

Equally valid alternatives may result from open discussion within the Police, the Judiciary and the Legal Profession. However it may come about, there is no doubt that some action is vital.

Within the United Kingdom at the moment, case law concerning computer evidence is still very scarce. There have been few signs yet that incompetent, irrelevant or frivolous expert testimony has materially affected the outcome of proceedings but considering some of the examples mentioned above, it seems only a matter of time before a high profile case is irredeemably compromised by irrelevant technical confusion. If that happens all computer forensic experts may become tarred with the same brush and the work of all of us will become that much more difficult. ■



Book Review

Computer Crime: *A Crimefighter's Handbook*

by David Icove, Karl Seger & William VonStorch.

O'Reilly and Associates Inc., Suite A,
103 Morris Street, Sebastopol, California,
95472, US.
437pp. £20.50 sterling.

The authors have produced a jargon free and eminently readable book. This is a useful guide for newcomers to forensic investigation, but includes more detailed information for the expert.

'Computer Crime' is divided into three sections, the first dealing with high-tech crimes and the people who commit them, including profiles on computer criminals, and the laws relating to crimes.

The second section is proactive and gives information about preventing computer crime. Areas which are covered include aspects of security including personnel, communications and operating systems.

Section three gives information about handling computer crime from discovery through forensic investigation, to prosecution of the criminal. This section includes suggestions for gaining evidence of the crime and offers advice to investigators testifying in computer crime cases.

There is a substantial section dealing with computer crime law which, although mainly relating to federal and state laws in the US, has useful reference to European and other countries.

The book has comprehensive appendices, which provide extra information on books, periodicals, user organisations, electronic resources etc., and has a substantial, and very useful, glossary. This book is a fascinating read and is an excellent introduction to all aspects of computer security and crime. ■

Reviewed by: Ray Hatley

Profile

Patrick Lantin

Information technology consultant Patrick Lantin works closely with the Belgian justice department and is a computer expert with the European Commission. He is involved in investigating all kinds of computer-based crime as well as helping to fight the threat of software piracy.

Lantin, 40, is a freelance computer detective who undertakes investigations in both the public and private sectors. He has seen a marked growth in computer-related crime in recent years, culminating with the recent paedophile scandal which shocked the world. Until June last year Lantin was vice president of Dr PC, the worldwide on-site computer assistance firm, and he has built up his experience from nine years of hard work in the field. His duties now include giving close computer support to a wide range of judicial investigations, including drug crimes, fraud and software piracy and counterfaking.

But while the technical experts do their best, Lantin fears the legal system is a weak link in the chain, with judges still not fully up to speed on the potential that computer forensics can offer. Lantin said: "It can be very frustrating. Some of those in the legal profession were not brought up with computers and the possibilities they offer and are only now beginning to understand them. It's a world wide problem. Hopefully this situation will change very soon. The Belgian justice department has announced that 525 judges and officials will get a computer and a three-day training course. This should make them more computer literate. And because computers are quite new and are always changing and improving, the laws in Belgium don't really take them into account properly. Computer crime is relatively low in this country at the moment, but will greatly increase very soon. It's not much good being able to get evidence from computers if it is then not used properly in court. Computers are becoming more and more important in any investigation."

Lantin fears the recent paedophile scandal has created an atmosphere of fear. He said: "It's made everyone absolutely paranoid, creating a very dangerous situation, with more than 15 privately owned paedophile announcement sites on the Internet. It's like a witch hunt, but fortunately things are improving now."

Much of Lantin's work is with private firms who need to get to the root of a problem, often fraud, without the embarrassment and publicity involved in a police investigation and trial. He said: "Often companies don't want everyone to know what has been going on, and just want to find the culprit. I would like to see a private service to look at crimes related to information technology in the commercial sector.

"The potential is great in many businesses for computer crime and fraud. Often accounts and records of financial transactions are held on computers, and it's important that firms are aware of the dangers and how to solve problems when they arise." And as computer crime increases, Lantin says there should be greater links and co-operation between countries and individual investigators. He said: "I would like to see a world wide IT fraud centre to exchange experiences and related software, and for the close collaboration of international services. It's very important that we all talk to one another. It would also be a good idea for universities to start new courses which would cover both the law and computer technology, that way we would have many more people with exactly the right training." ■

*** The views expressed are not necessarily those of the Belgian justice department.**

When is a PC not a PC?

The Forensic Examination of Commodore Amiga Computer Systems

Most of the procedures developed for the forensic examination of personal computers have one distinct drawback - what happens when the computer being examined is not an IBM PC compatible computer?

In the modern Microsoft/Intel dominated industry it is easy to forget there are other systems available. The Apple Macintosh system is still a popular choice and there is plenty of experience in the forensic world for dealing with this format. But there are other systems apart from the PC and the Mac, and one in particular is still in widespread use throughout Europe:

During the early 1990s the Commodore Amiga was the most popular home computer in the United Kingdom, selling over two million units. With its fast, low-overhead multi-tasking operating system it became the machine of choice for many bulletin-board systems, even those not specialising in Amiga matters.

Even now, three years since the demise of Commodore who manufactured the computer, the level of enthusiasm for this computer system is remarkable, and various companies are producing Amiga-compatible computer systems. While the heyday of the Amiga has long since passed, there are still many machines being used on a daily basis. Inevitably a small number of these end up in the hands of the investigating officer during the course of an investigation.

The Amiga system offers many problems to the investigator who is more used to IBM PC systems.

Firstly, during search and seizure, the Amiga may well be overlooked. Most Amiga models are designed to hook up directly to a standard television, and may well be left in cupboards or boxes when not in use. One variant, the CDTV system, looks like a VCR or Compact Disc player, and could be placed in a hi-fi stack or under a television and remain unnoticed by the investigator. The three most popular models, the Amiga 500, 600 and 1200, have the CPU, disk drive and keyboard in one unit, an extended keyboard with a slot for the 3.5" disk on the right hand side - there is no separate system box to search for (although other Amiga models do have a more traditional layout with separate keyboard).

Almost everything about the Amiga is non-standard, when compared to an IBM clone computer. Although it utilises standard IDE or SCSI hard drives and standard 3.5" diskettes, the disk format used on Amiga devices is proprietary and cannot be understood by any standard PC forensic examination tool - Amiga formatted diskettes are physically impossible to read, except on an Amiga disk drive.

Most Amiga models require special monitors (capable of 15Khz horizontal and 50Hz vertical frequency) if not being connected to a video monitor or television. Keyboards and mice are also non-standard. An attempt to plug in a standard PC mouse and keyboard to an Amiga system could result in damage to the system.

Examination of Amiga systems is difficult at best. Standard procedures can be used to create a mirror image of the hard drive(s), but these mirror images are virtually useless to the investigator as the Amiga file systems (of which there are several, including some which employ Stacker/Drive Space style compression) are not readable on any pc device, and have to be examined on an Amiga system.

The Amiga can be configured to read/write standard PC 720Kb (and 1.44Mb on the high-end systems) diskettes for transferring data. However, in forensic investigation we have found that the most practical method of bulk examination of data is the transfer of all files from the hard drives to recordable CD-ROM disks in standard ISO-9660 format. While this does not record all the potential evidence from the disk (as is the case when making a complete mirror image), it does provide the data in a format that can be examined on a standard PC forensic workstation thus allowing the examiner to locate files and directories of potential interest. These can later be examined more thoroughly on an Amiga system set up to run image duplicate hard disks of the original system.

Locating deleted files and file fragments on the Amiga requires special software, standard forensic tools being unable to understand the Amiga file system structure. Fortunately there are several packages available for this task, but again this needs to be done on an Amiga-based examination system.

Investigations on the Amiga are a challenge; I have little doubt that many people choose Amiga systems because they think enforcement authorities may be unable to investigate such systems. However, successful prosecutions recently in the UK have shown this is not the case - and evidence on Amiga systems, even complex systems with multiple CPU boxes and many hard drives, has been recovered and used successfully in court. ■

By Jolyon Ralph

Jolyon Ralph is recognised as an Amiga Forensic Expert; he works closely with police investigators. He is Technical Director of Almathera Ltd, Mitcham, Surrey, UK. Tel: +44(0)181 687 0040 or e-mail: jralph@cix.compulink.co.uk. URL:www.almathera.co.uk

Floppy Disks - not a problem

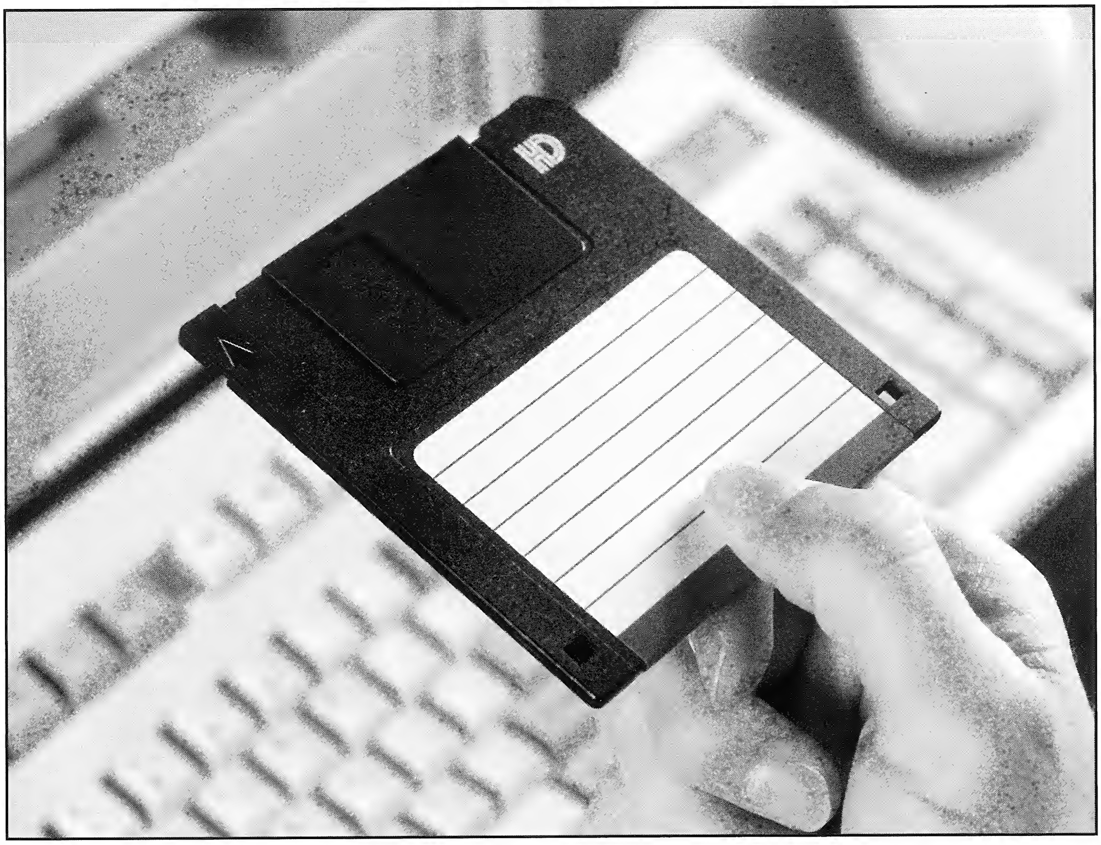
With supersonic processor speeds and stratospheric disk sizes; with ZIP disks, JAZZ disks, CDs, Opticals, WORMS, DVDs and heaven knows what else the industry is about to present us with, hard pressed investigators could perhaps be forgiven for forgetting the humble floppy disk. However, they're still with us and they can still hold the key you might be looking for.

Sometimes a floppy disk may be central to the investigation - all of the technical evidence in the AIDS Disk incident in 1989 was found on just two 5¹/₄" floppies; vital evidence that helped to convict the Black Baron virus writer in 1996 was found on a single 3¹/₂" floppy disk; even a current investigation hinges on the contents of floppy disks found concealed behind a picture. Sometimes the evidence is peripheral - like the captured datastream information transferred on floppy disks by the Hole in the Wall Gang in 1996. Floppy disks are a universal, cheap and convenient method of data storage and for the criminal they may represent an extremely easy way to store and hide vital but damning information - the investigator ignores them at his peril.

Investigating the content of one or two floppy disks presents no new difficulties and is not a problem as long as an established procedure is followed. However, new problems will surface as soon as the quantity of disks increases. Past cases have involved detailed investigation of 1,700 and 1,900 assorted floppies respectively and while such numbers will represent no more than about 2 gigabytes of data, the fact that the data is fragmented over such a large number of slow access devices can become an investigator's worse nightmare. Consider a money laundering operation involving hundreds of different companies dotted around the world. Transactions to and from individual companies are located on different floppies and investigators are faced with the gargantuan task of reconstructing this financial web by constant reference through hundreds, maybe thousands of floppy disks. Even just copying them can consume valuable resources - a good operator will take at least 3 hours to copy and document one hundred floppy disks and that is assuming no tea breaks and no errors! Happily there are now floppy imaging programs which enable mass copying, examination and analysis on faster, high capacity storage media and this has greatly simplified at least some of the problems.

Floppy Disks: The Background

Floppy disks as we know them have been around virtually since the first commercially available computers in the early 1970s. There were a number of early disk sizes on personal computers but in the late 1970s the first standard was set with a disk of 5¹/₄ inch in diameter, recorded on one side only. The early 1980s saw the introduction of the IBM Personal Computer and that used a 5¹/₄ inch disk recorded with 40 tracks of information each containing 4,096 bytes of data. Each track was divided for reference purposes into 8 sectors of 512 bytes giving a total disk capacity of 163,840 bytes (=160Kb).



Improvements in technology soon allowed the capacity to be increased - first by making the drives capable of reading and writing to both sides of the disk (giving 320Kb capacity) and then by increasing the amount stored on each track to 4,608 bytes (9 sectors). Single - and double - sided disks of both 8 and 9 sectors per track can still be found today giving total capacities of 160Kb, ▶

Capacity	Tracks	Sides	Sectors per Track	Diameter
160Kb	40	1	8	5¼ inches
180Kb	40	1	9	5¼ inches
320Kb	40	2	8	5¼ inches
360Kb	40	2	9	5¼ inches
720Kb	80	2	9	5¼ inches
720Kb	80	2	9	3½ inches
1.2Mb	80	2	15*	5¼ inches
1.44Mb	80	2	18*	3½ inches

Figure 1

180Kb, 320Kb and 360Kb. The next development involved improving the surface coating of the disks so that 7,680 bytes (15 sectors) could be stored on a single track and at the same time the width of each track was reduced so that 80 tracks could be stored instead of 40. This gave a capacity of 1.2Mb but required special drives that could recognise the different coating and switch their reading capacity between the different data densities. These new drives could be persuaded to read and write 80 tracks at the lower density on the older type disks and so a 720Kb format came into being (double sided, 80 tracks, 9 sectors per track). This was never officially accepted as a standard but since the 1.2Mb disks were prone to errors and were extremely sensitive to mistreatment, the 720Kb disks gradually grew in popularity amongst the computing enthusiasts.

The next development produced a more robust disk supplied in a rigid plastic case. These were 3½ inches in diameter and although the principle (and the number of tracks) remained the same, the quality of the coating on a better protected surface allowed a similar data density even though the disk was smaller. Technology improved rapidly and it was soon possible to buy better quality 3½ inch disks which could reliably store 18 sectors per track (giving 1.44Mb storage). Throughout this development, the division of each track into 512 byte sectors has remained standard. Recently, even more highly refined disks have become available with a capacity of 2.88Mb but as fixed disk technology has improved and become cheaper, the use of floppies has declined and the 2.88Mb disk has not achieved the universal acceptance of the 3½ inch, 1.44Mb disk.

In recent years, some enthusiasts have attempted to pack more onto existing floppy disks by increasing the number of sectors per track. This has created a number of non-standard formats on capacities ranging from 1.5Mb to 1.9Mb but the practice is not widespread because special software is needed to read and write data on such disks and the reliability falls off rapidly as the data is more and more densely packed. So the currently accepted formats can be summarised in a table *(see figure 1)*.

Practical Considerations

As each of these capacities came into use during the 1980s and early 1990s, a number of anomalous conditions developed which stemmed from the differences in data density. Note that in the above table two entries are marked with an asterisk *. These disks had a coating with a much finer particle size and could store data more densely. Unfortunately they needed slightly different recording currents and so it was necessary for the drive to recognise the disk type and change its operating conditions accordingly. On the 5¼ inch disks this was done electronically and was not very successful. On the 3½ inch disks an additional hole was placed in the disk envelope so the drives could use that as a density indicator. The range of drive mechanisms available to computer users was vast and some were unable to correctly recognise the media. This meant that the drive might attempt to write a high density format to a low density disk and errors were generated which increased in the higher track numbers.

This comes about as follows:-

The angular velocity of a disk is fixed by the drive speed at around 360 r.p.m. but if we consider the linear velocity - the speed at which the media passes the head - this decreases with the tracks nearer to the hub. Track 0 is always the outside track and if this is 2½ inches from the centre the track is 15.7 inches long (π x 2½ x 2). Track 80 is nearest to the hub and if this is 1¼ inches from the centre then the track will be 7.85 inches long (π x 1¼ x 2). Since one track passes in one revolution of the disk (1/360th of a minute) the linear velocity of the outside track will be 15.7 inches in 1/360th of a minute or 94.2 inches per second. The inside track will only be half this at 47.1 inches per second.

The effect is to produce a disk which appears to be 1.2Mb (or 1.44Mb on 3½ disks) but which has a large number of clusters marked as unusable such that its available capacity is much less. This can still mean more storage than the lower density would allow (typically up to 900Kb) but has the risk of some of the data being unrecoverable. From a non-technical user's point of view the disk appears slow but otherwise functions normally. When the forensic investigator encounters such disks he needs to copy them (errors and all) onto correct media (disk or image) so that subsequent examination is as accurate as possible. ■

Case Studies

Logic bomber

An IT manager had threatened to plant a logic bomb on his company's system unless he was paid a substantial sum of money. He was already suspected of disrupting the computer network as well as sending anonymous hate mail and threats.

Technicians broke into his computer which was heavily protected by a series of passwords as well as software and hardware tripwires and boobytraps. A disk image was subsequently analysed upon which resided a wealth of incriminating evidence. The suspect was also caught on camera in the act of disrupting ethernet connections. On being presented with the computer evidence, the suspect signed a statement of his complicity.

Technical notes

The suspect was monitoring the access control logs which recorded people's entry, exit and movements within the building. It was necessary, therefore, for the investigation team to edit the access control log-file so that its activities would not be disclosed. A covert video system activated by a Passive Infra-Red (PIR) monitor was placed in the computer suite where physical disruption of cabling was suspected. This camera was activated by the appearance of a significant heat source (e.g. a person) in the area of surveillance. The PIR activation reduced the hours of recorded material; for evidential purposes the video tapes were digitally dated and time stamped.

The BIOS password on the suspect's IBM PS/2 was circumvented by slaving the hard disk from his machine to another PS/2 to which the password was known. The "donor" machine was booted from a DIBS 3.00 disk (Computer Forensics Limited) and the imaging (using the Disk Image Backup System) commenced without further problems. There was no need to use CMOS setup software or auto-seeking in order for the DIBS software to recognise the slaved hard disk type and parameters.

The advantage of transplanting the hard disk was that the suspect's password was retained in CMOS; he therefore had no reason to suspect that his computer had been accessed when he reported for work the next day. Two images were taken. The primary DIBS image, recorded on a Panasonic optical disk, was examined locally in a hotel room using a laptop computer. Incriminating documents and data fragments were printed out. The secondary image was maintained as a control. Images were dated, time-stamped, with computer make, model and serial number and witnessed.

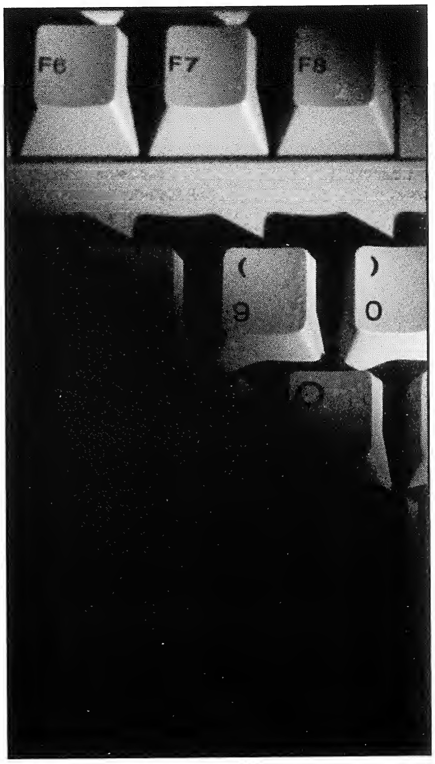
Interestingly, had the investigation team entered the computer using the suspect's password, a TSR spy program would have been invoked by AUTOEXEC.BAT. This TSR would then have recorded all resource usage including the date and time that software items were executed to a hidden file. Fortunately, the investigation team never knew the suspect's password and did not blunder into this ambush.

AUTOEXEC.BAT file invoked a keyboard monitoring program as soon as the PC was powered up. In this case, the computer had been set so that it could not be booted from a system diskette. An attempt to examine the computer via the "front door" would be revealed to the suspect. If conducting a covert investigation it is important not to guess passwords. Certain CMOS types record invalid logins including the date and time of the attempt, and echo this to screen when the PC is next powered on. The suspect would thus be alerted by the following login screen when he next uses his machine:-

```
XXX Invalid Password XXX
Sun 04-23-1995
11:32:09pm
ENTER PASSWORD_
```

Approximately seventy diskettes were copied using DOS diskcopy on a non-evidential laptop (i.e. not a computer used by the suspect). Sixty Polaroid instant photographs were taken and used to restore the search area following the investigation. The investigation team wore forensic gloves for handling diskettes and documents as it was believed possible that fingerprint evidence might be needed - this was in fact not necessary. The covert desk search, computer data backups and installation of the camera were completed between 11pm and 5.30am.

Covert investigations require very careful planning and preparation. In this case information about the suspect's work area and his computer was ascertained prior to the search. On his return to work the next day, it was evident that the search team had left no indication of its night-time activities. ■



Investigating Floppy Disks...

When investigating floppy disks, particularly in large quantities, it is essential to stick to an established procedure. Of course it is possible to write protect and examine disks directly but floppy disks recovered during a search may be old or dirty and they should be handled with extreme care.

The careful investigator will not read them more than is absolutely necessary to collect the information that they contain and this will entail copying them just once - onto other disks or into files containing a copy of every sector (called image files). If the quantities are large (in excess of fifty or so disks) copying to image files is the only practical alternative. Once copied, the original disks can be securely sealed in evidence bags and stored. These will constitute the best evidence and at the direction of the court can be opened for examination in the event of a dispute. All subsequent work is performed on the copies and any evidence discovered will refer to a numbered image file. The following procedures have been found very effective in practice:-

Sorting

Floppy disks are normally placed in sealed evidence bags as they are discovered during the search, and each bag will be labelled with an exhibit reference number. The number normally refers to a specific location allocated at the search site. When the investigator receives the bags, each is treated individually. A note is made of the bag's seal number and the bag is opened. The disks are sorted manually according to size and density, and attention is paid to individual labels so that disks with consecutive numbers such as Backup 1, Backup 2 etc. are sorted into sequential sets. Each disk is then copied to an image file within a specially created directory and any which appear unformatted or non-DOS are placed on one side for later attention. Disks which are successfully imaged are numbered to match the image file number and returned to the evidence bag for eventual resealing. Any non-DOS disks are numbered and bagged separately after attention and the whole exhibit group can then be resealed with a new seal number. Thus in the event of any dispute, evidence located in a particular image file can be directly referred to the original disk in the newly sealed bag.

Media Preparation

Floppy disks are copied onto either an optical cartridge or a fixed disk. On either type of media a number of sub-directories are created numbered D1, D2, D3 etc. Into each of these sub-directories a maximum of 100 floppy disk images will be created. As each disk is copied, the image file is automatically numbered within its own sub-directory. Thus a two part reference is created D1/001 to D1/999 or D2/001 to D2/999 etc. and this is written onto the disk using an indelible pen.

Copying

As each disk is copied, the details are written to a recording sheet laid out as in *Figure 1*.

The exhibit number is written into the Disk Reference column. Details of the label are written in the third column and any pertinent comments are recorded in the fourth column. A completed sheet may look something like *Figure 2*.

Each sheet has 25 rows and there are four sheets to each sub-directory. Each disk/image number is checked three times during the copying process and the total number of disks copied is checked continuously by comparing numbers of sheets with numbers of floppies copied.

The copying software keeps a record of any errors encountered and for each image file this record is available for reference during subsequent examination and analysis.

Examination

Once the copying process is completed, the investigation can begin and will usually follow similar procedures to those laid down for fixed disk examination. ■

Image Number	Disk Reference	Label Details	Comments
D1/001			
D1/002			
D1/003			
D1/004			
D1/005			
D1/006			

Figure 1

Image Number	Disk Reference	Label Details	Comments
D1/001	ABC/23	Backup 1 of 3	Errors
D1/002	ABC/23	Backup 2 of 3	
D1/003	ABC/23	Backup 3 of 3	
D1/004	ABC/23	(No label)	Damaged shutter
D1/005	ABC/23	Alan's Letters	
D1/006	ABC/24	Mike's Accounts	

Figure 2

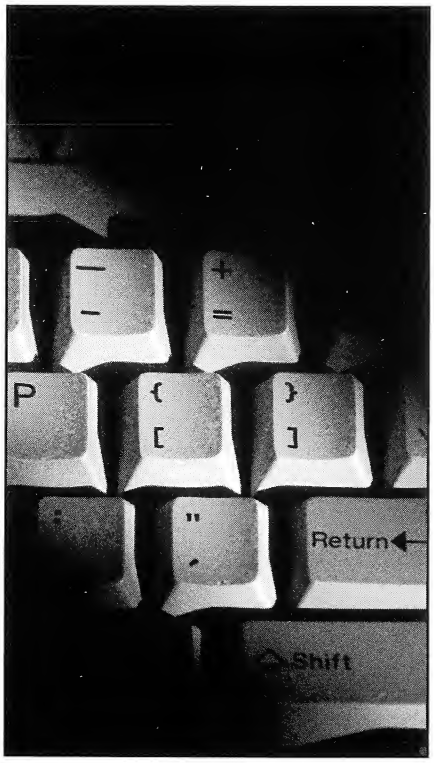
Anonymous Letters

Some highly damaging computer generated letters had been posted to the major customers of a client causing a failure of confidence and tangible commercial loss.

Contextual analysis indicated that these letters had been written by a particular individual in a sales department. The computer's hard disk was copied and the text of the anonymous letters was searched for at sector level using a multiple string search engine. Two of the letters were found in the Windows swap file - a hidden system file which many computer users do not know exists. Ironically, the author of the letters (who subsequently confessed) had used the Norton Utilities to irrevocably destroy the original computer documents but had failed to appreciate the subtler intricacies of the Windows user interface.

Technical notes

The Windows swap file, 386SPART.PAR, is a hidden system file found in the root directory of PCs running Windows 3.1. Usually a large file (often exceeding 20 megabytes), 386SPART.PAR records resource usage, printer queue information and, crucially, proprietary information which is processed during each Windows session. This means that it is possible to extract evidence even when a suspect has not actively saved the file to disk. In one instance, a memo had been written on screen and printed but not subsequently saved - its contents were found in the swap file. Windows 95 also has a swap file WIN386.SWP which resides in the sub-directory C:\WINDOWS.



In this case, contextual analysis was more important than any computer wizardry. By analysing the content of the hard-copy, particularly with regards to motivation, content, punctuation, syntax, style, layout and other contributory factors the prime suspect was quickly identified. Postmarks, stationery, indentations and forensic matters relating to Questioned Document (QD) examination may also prove helpful in investigating the source of anonymous letters.

Once the suspect's computer had been identified, an image was taken and a multiple string word search was executed using Sweep (v.2.64) from Sophos plc. (Note: later releases of Sweep are ineffective for this sort of search.)

As an observation, the Norton Utilities, PC Tools, PGP encryption and a range of powerful software utilities are often found on suspects' disks. If properly used they would make the work of the computer investigator practicably impossible. Fortunately, experience has shown that these tools are rarely used or are used somewhat incompetently. As an example, one suspect encountered by the author had high level formatted the partitions on his hard disk unaware of the fact that the high level format command (typically FORMAT C:) is non-destructive. ■

The above Case Studies are provided by ***Edward Wilding****, Senior Consultant at Network Security Management Limited ("Network"), a subsidiary of the Hambro Banking and Financial Services group. Network is a specialist company with headquarters in London which investigates white collar crime and fraud on behalf of corporate clients worldwide. Wilding may be contacted at the following address: edward@nsml.com, Compuserve 101377,2675.*

Figure 1.

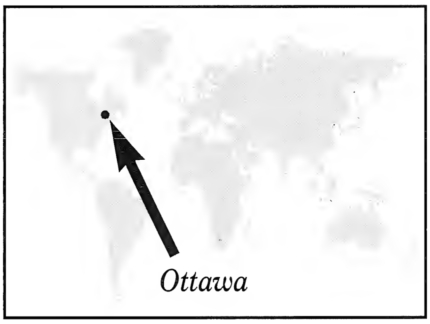
Once a suspect is identified, his or her computer and disks should be examined using a sector level search. The discovery on a DIBS image is definitely not a false-positive.

```
The scanner report...
Examining area 1: d:|*
>>> Pattern 'Rather than' found in sector 3862 of drive D:
>>> Pattern 'poking' found in sector 3862 of drive D:
>>> Pattern 'around in' found in sector 3862 of drive D:
>>> Pattern 'accounts,' found in sector 3862 of drive D:
>>> Pattern 'you should' found in sector 3862 of drive D:
>>> Pattern 'concentrate' found in sector 3862 of drive D:
>>> Pattern 'on John' found in sector 3862 of drive D:
>>> Pattern 'Smith in' found in sector 3862 of drive D:
>>> Pattern 'purchasing.' found in sector 3862 of drive D:
>>> Pattern 'This' found in sector 3862 of drive D:
>>> Pattern 'bastard' found in sector 3862 of drive D:
>>> Pattern 'is ripping' found in sector 3862 of drive D:
>>> Pattern 'the company' found in sector 3862 of drive D:
>>> Pattern 'off. Check' found in sector 3863 of drive D:
```

Old Laws, New Crimes...

...and a Shrinking Planet

Hindrances in the Investigation of Computer Related Crime



There exists a special kind of journey that takes only milliseconds to complete - a trip on the information highway - and such a trip, if it involves criminal activity, can have enormous implications for law enforcement agencies everywhere in the world. Such transactions are often silent and undetected; they cross international borders with ease and speed; and, evidence of their existence can be easily concealed. If such a crime is initiated in Canada but lands on a foreign doorstep, which country's laws apply - our's or their's - if, in fact, we have laws that apply at all?

Such are the questions raised - and raised with increasing urgency - as sophisticated computer crime threatens to outpace our ability to deal with the technological revolution that is changing the world in these last years of the twentieth century.

Technological growth has progressed at such a hurried pace in the last few years that many of us would believe it has outstripped the development of criminal legislation. There are gaps in domestic law and in international co-operation and these have caused problems in the investigation and prosecution of both traditional and computer crimes.

There is much evidence that organised crime is beginning to gain a strong-hold in computer crime. New computer and communication technologies are being used to quietly launder the profits of crime and this is being accomplished with almost certain assurances of anonymity.

Old Laws, New Crimes, and a Shrinking Planet

"Old Laws, New Crimes, and a Shrinking Planet" relates to some of the hindrances that exist in the investigation and prosecution of computer related crime. Canada has already achieved a considerable amount of success, both domestically and internationally, in dealing with this most troublesome problem. Much remains to be accomplished and a lasting solution to this problem may prove elusive unless the global village comes to grips with the many issues that now confront all of us.

OLD LAWS
Definition of Criminal Conduct

It is generally agreed there are two forms of computer crime: The first involves the computer as an instrument to commit traditional crimes. The second involves the computer as the object of abuse. An example of the first may be a bank employee who uses a computer to transfer bank funds to a private account and then disappears with the funds. The second might have that same disgruntled employee sabotaging the bank's computer system by erasing, destroying, or altering the data contained therein.

In Canada, very few problems have been encountered in the prosecution of cases where the computer has merely assisted in the commission of traditional crimes such as fraud and theft. Canada has created computer specific offences that make it an offence to use a computer in an unauthorized manner (Section 342.1 Criminal Code), or to commit mischief to data (Section 430 Criminal Code).

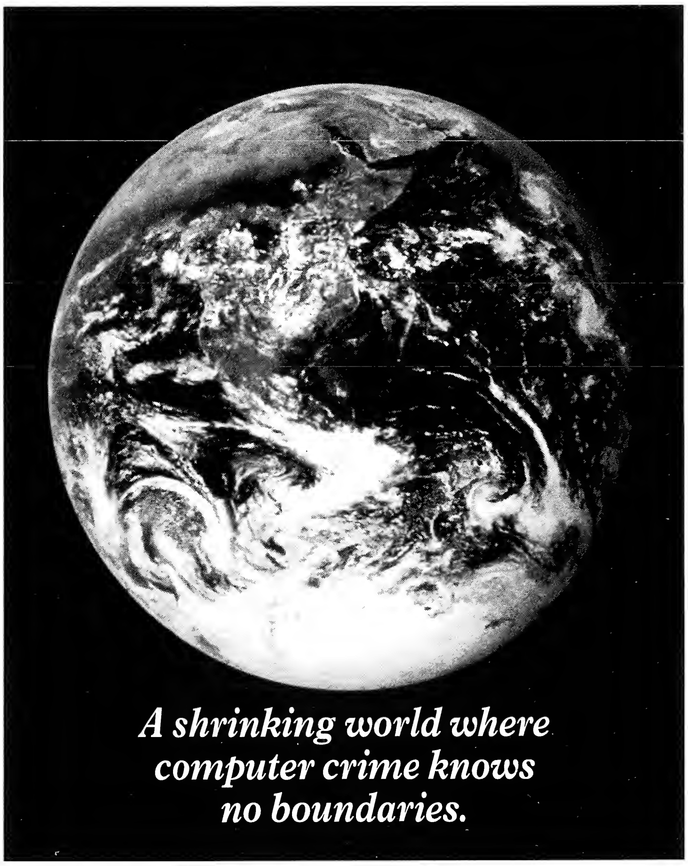
The RCMP has developed its own definition of "computer related crime" by extracting and then combining the basic elements of these computer specific offences:

"Any criminal activity involving the copying of, use of, interference with, access to, or manipulation of computer systems, computer functions, computer data, or computer programs."

Internationally, there appears to be a lack of consensus as to what constitutes a computer crime and what types of abuses should be criminalised. Theses uncertainties have created problems in international co-operation, especially where dual criminality is required to satisfy requests for international assistance.

Search and Seizure

Searches of computers can extend to computer systems that have not been specified in search warrants. Obtaining a separate search warrant is not always possible because of time constraints. For example, a search of a computer at one location can lead to the identification of a connected computer at a second location. After police have conducted their search at the first, that custodian could instruct the operator of the connected computer to delete the data sought by the police. Functionally, the police are able ▶



A shrinking world where computer crime knows no boundaries.

to obtain secondary search warrants for domestic cases involving extended searches. When extended searches transcend national borders, it may not always be practical or legal, for that matter, to conduct a search in a foreign jurisdiction.

Interconnected computers provide for the storage of static data and the transmission of moving data. Legal differences can exist between the traditional powers of search and seizure and the rules associated with the interception of communications. Electronic and voice mail are two examples where these characteristics appear to overlap.

Increased Court Challenges

In Canada, court challenges concerning the integrity and authenticity of electronic evidence have increased. This may be the result of persons charged being more computer literate or having high skill levels; counsel for accused persons having gained computer expertise; more legal precedents having been established; and, the laws not having kept pace with technological growth.

At the Second International Law Enforcement Conference on Computer Evidence in Baltimore, Maryland, the point was made that it will be incumbent on law enforcement agencies to devise generally-accepted practices, procedures, and principles for the collection and presentation of computer evidence. Our failure to develop standards could result in the courts imposing their own rules that might not always prove popular among investigators.

NEW CRIMES
Technological Advancements

Computer crime goes hand-in-hand with changes in technology. A question is now being asked by those of us in law enforcement: What is the future threat posed by computer crime? The only true answer is that no one knows. In few other fields of law enforcement are we faced with quite the same degree of uncertainty. A break and enter today will probably be very much like a break and enter six years from now. But a computer crime six days or six weeks from now may be totally different altogether. The exact threat will be in direct relationship to advances in technology at any given time.

Training Requirements

Law enforcement training has not always kept pace with changes in technology. In addition, computer training is broadly based and requires knowledge in many different disciplines. Investigators must be encouraged to keep abreast of changing technologies and to participate in developmental or refresher training.

Computer crime and the use of computer technology are now evident in many other areas of criminal activity such as drug trafficking, the counterfeiting of payment cards, illegal gambling, and loan-sharking.

Few investigators have the proper combination of investigative experience and technical ability and even fewer have the necessary experience to deal with such a wide range of activities. As well, few investigators have an adequate understanding of the international issues such as extradition and mutual legal assistance treaties.

The intangible nature of computer data and other related issues have resulted in the need for training that differs considerably from traditional training provided in search and seizure techniques. The large storage capacity and speed with which computers operate also give rise to difficulties in the detection of crime. Computer crime and the use of computer technology can be sophisticated and criminals often possess a high skill level. It will be necessary that investigators possess comparable degrees of skill level.

Quantitative Statistics

In Canada, it has been difficult to obtain quantifiable statistics relating to incidents of computer crime. Our crime statistics do not necessarily portray an accurate picture of computer crime activity in Canada since the vast majority of cases have involved traditional offences where the computer has merely assisted in the commission of a crime.

Other difficulties have occurred in our efforts to quantify computer crime. Perhaps the best known of these is the "dark figure" phenomenon which accounts for those computer crimes that are not reported to police for a variety of reasons (eg adverse

▶

publicity, corporate embarrassment, loss of goodwill etc) and are intrinsically linked to bottom-line issues.

SHRINKING PLANET

Jurisdictional Problems

Telecommunication and computer communication systems can transcend many national borders. Since computer crime knows no boundaries, significant problems have resulted in determining which jurisdiction should assume prosecutorial responsibility.

Jurisdictional problems arise in crimes committed on global networks such as the Internet. The wilful promotion of hate propaganda is a criminal offence in Canada. If a hate monger in Canada was intent on communicating his/her message, that person need only establish an Internet distribution site for hate literature in some other country where the laws are more permissive. This would provide Canadians with the means to download the material from the foreign Internet site and because the site would be located outside of Canada, little action could be taken by Canadian authorities to prevent this kind of activity.

International Co-operation

Stand-alone computers have been replaced by computers interconnected by networks and interconnected networks. Computer crime has truly become a global concern and co-operation to the fullest extent possible is both desirable and necessary.

Canada, through its involvement in Council of Europe discussions on information technology, suggested that international agreements be negotiated to ensure that expedited and adequate procedures exist to seize data in foreign countries under special circumstances. One such proposal called for the creation of a mechanism similar to that used when seizing documents from a lawyer over which a solicitor-client privilege has been claimed. In such cases, the documents are seized and are immediately placed in a sealed packet. The packet is delivered to the custody of the courts and a hearing is held before a judge to determine whether the contents of the package should be disclosed and returned to the police officer who seized the documents in the first instance, or whether they should be re-sealed and returned to the lawyer. It is possible that a similar process could be applied to exigent computer search and seizure procedures in foreign jurisdictions.

Harmonization of Criminal Laws

Canada, in its recent presentation to the P-8 Senior Experts Group on Trans-national Organized Crime, recommended that further consideration be given to the harmonization of laws through the negotiation of an international convention. Such a convention would obligate countries to criminalise certain types of computer related abuses and would resolve many of the jurisdictional and procedural problems that currently exist.

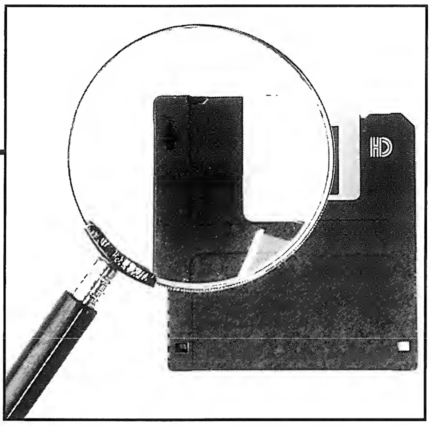
Conclusion

Canada and its international partners have already achieved a good measure of success in limiting the threat posed by computer crime. Nonetheless, there is still much work to be done. Law enforcement agencies have played, and should continue to play, an important role in finding solutions. For in the end, it will be common initiative, common input, common interest, and in short, the co-operation of the whole of the global village that will ultimately ensure our final success. ■

This article was written by

Cpl. Michael Duncan *of the Royal Canadian Mounted Police, Technological Crime Section, Ottowa, Ontaria and is reproduced here with the kind permission of RCMP Gazette.*

Forensic Q&A



Q *I have seized a mobile telephone during a raid. How should I handle it and can I access the numbers stored on it?*

A When a mobile telephone is seized, switch the telephone off to preserve the continuity of the evidence. Take care that numbers on the key pad are not pressed, as this could lead to the loss of any evidence stored. If a mobile telephone has an address book and last number re-dial facility, the data will be stored within a subscriber identification module (SIM) card. Many police forces have a single point of contact, often contained within a force intelligence bureau, to deal with all such enquiries. They should have the specialised equipment required to access the card.

In commercial organisations, the investigator will need to obtain advice from the mobile telephone network provider. The service provided differs between networks. Some may charge for this service.

Q *I have a number of phase change optical cartridges which I have used in cases which are now finalised. Is it acceptable for me to re-use these on new cases?*

A The current procedure for using optical cartridges is that for each copy the manufacturer's seal on a new cartridge is broken just before the data transfer takes place. This is intended to ensure that no information from another investigation could be on the cartridge. This procedure is based on that used for audio and video tape.

From a technical viewpoint both optical cartridges and magnetic storage media can be reformatted and re-written in such a way that it is quite impossible for any previous information to remain, or to be recovered. With magnetic media the organisation of the ferrous particles, the pattern of which is used to store information, can be returned to a uniform state by application of a suitable magnetic force. However, the low cost of magnetic media does not justify the time taken to complete the process. It is more cost effective to use a new tape. With phase change optical cartridges the re-writing method used during the reformat process is essentially a chemical process that cannot be reversed. It is analogous to the process of taking a car body and melting it to reform the piece of steel from which it was originally created. Although the resultant material is the same, the reheating process cannot be reversed to recreate the original body shape. The relatively high cost of the media and the small amount of time taken to reformat and re-write makes the process economically viable.

From a legal and procedural viewpoint, however, the re-use of optical media may not be advisable. The current guidelines regarding optical media use are the same as those tried and accepted in court for magnetic media. Some police forces within the UK are currently examining the re-use of optical cartridges and whilst there is no technical reason why an optical cartridge should not be re-used the concept will need to be tried, tested and accepted by the court.

Q *We have seized a computer in a raid which is an Apple Mac. All my experience is with PCs - do I copy and examine this in exactly the same way?*

A Apple Macs resemble PCs in the structure of the hard disk in that they have allocation units of a set size, into which files are saved. However the way in which files are constructed within a Mac is very different from that in a PC. The applications used to create different file types are not separate from the files themselves. When a file is selected and opened the application linked to that file type is loaded automatically. On the hard disk the information pertaining to a specific file is kept in a single place. When additions are made to files/directories, a marker indicates the new location of that file on the hard disk.

The hard disks within Apple Macs are usually attached via a SCSI interface. The hard disk within the Apple Mac is seen as the first SCSI device attached to the machine. The Mac can be forced to ignore its internal hard disk and boot from an external SCSI device which includes an appropriate operating system by using a specific sequence of keys on the Mac keyboard: COMMAND + OPTION + SHIFT + DELETE. Although you have instructed the Mac to ignore its internal hard disk, there is still a possibility that information could be written to the hard disk during the checks for attached SCSI devices during the boot process.

If a second external device, which could be a SyQuest drive or optical drive is then attached, a block by block copy of the hard disk can be obtained by using an appropriate utility. An alternative is to remove the hard disk from the Apple Mac and insert it into the hard drive of a PC equipped with a SCSI interface; it can then be copied as normal. The copy of the hard disk thus obtained can be recreated onto a hard disk and then be viewed on a second Apple Mac. ■

Please e-mail your questions and / or comments to ijfc@pavilion.co.uk

Although every effort is made to ensure the accuracy of these answers, they are presented for general information and may not apply in rare specific cases. Readers are advised to seek confirmation from an independent specialist in forensic computing when dealing with evidentially valuable material.

Notice Board

EVENTS

Science and the Investigation of Serious Crime

16-17 April, Leicester, UK

Science plays an important role in the investigation of crime. Experts from a wide range of disciplines often can assist police enquiries, and provide crucial evidence in court. But, is the criminal justice system making the most of scientific expertise? What is the level of mutual awareness and understanding between scientists and other experts and those police detectives who direct and manage investigations. Just two of the questions which this two-day event aims to address.

Contact: Jerry Hart
Tel: +44(0)116 252 2471
Fax: +44(0)116 252 2783

International Police & Security Expo 97

1-3 July, Cardiff, UK
Tel: +44(0)181 313 3535
Fax: +44(0)181 468 7472

TRAINING

Computer Crime Consultants Ltd

are running the following course in April and May: *'Computer Crime - Incident Handling and Investigations'.*

This is a three day intensive course in investigative techniques and management.

Contact: Computer Crime Consultants Ltd
Tel or Fax: +44(0)1737 550093

Training in Computer Forensics

Four modules comprising:
Fundamental Computer Forensics
Applied Computer Forensics
Advanced Computer Forensics
Legal and Procedural Computer Forensics
Courses held monthly in West Sussex.

Contact: Computer Forensics Ltd
Tel: +44(0)1903 823181
Fax: +44(0)1903 233545

Reader's Response

Dan Mares of the US Internal Revenue Service writes:

In your January 1997 (Issue 1) Forensic Q&A section a person asked how to examine many floppy disks. Your response was to possibly use the DOS DISKCOPY command to make work copies of the disks.

I wish to point out, that copies made using DOS DISKCOPY are not 100% identical to the original. When DOS DISKCOPY makes a copy, it alters the serial number of the diskette. This is generally not a problem. But if the suspect had this knowledge they could create a program that looks for the original serial number, and if it is not found, the program will possibly decrypt the evidence. If the program does not find the proper serial number, (ie. a disk made with DISKCOPY,) then the program would provide erroneous results. This is not likely to happen. But I feel your readers should be aware that DISKCOPY "DOES" alter the copied disk. ■

Dan Mares e-mail: dmares@nocs.insp.irs.gov

Thank you Dan, you are correct but using DOS DISKCOPY to enable a preliminary examination of suspect material is generally quite sound. It should also be noted that the diskcopy facility within the Windows File Manager does not change the serial number. The assumption is always that the original material is preserved untouched (apart from copying) and can be referred to in the event of any difficulty.

Editorial Team

NEWS

The first of a new generation of digital storage devices, the Digital Video Disk or DVD, developed by Panasonic, will be available in the UK from April. Initially the system will only be used for accessing pre-recorded video and audio material on both conventional television receivers and existing personal computers. However, within two years DVD technology is expected to become fully read/write compatible and to provide a low cost, high capacity storage medium for all types of digital data.

The DVD system is an extension of existing phase change technology utilising a new fine focus red laser beam. This enables a high density of data tracks to be placed on the DVD and finer 'engraving' of the recording medium surface. The result is a single sided, single layer disk, virtually indistinguishable in size and appearance from a conventional CD, that can contain 4.7GB of data. Further development of the technology will result in a double sided, dual layer DVD with a data storage capacity of 17GB.

DVD drives for computers resemble existing CD drives and are expected to provide a low cost, high reliability replacement for existing hard drives and floppy drives. It is predicted that within three years personal computers containing huge DVD data stores will become standard.

For the computer forensic analyst, DVD technology will provide both new tools to be used in the investigative process and new challenges to be met in the analysis of ever larger quantities of computer data. ■

We will be pleased to receive contributions to this page. Please mark all correspondence 'Notice Board'. We reserve the right to edit if required.

International Journal of

FORENSIC COMPUTING™

Published by
Computer Forensic Services Ltd.